Department of Homeland Security Daily Open Source Infrastructure Report for 03 March 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Ohio state attorney general's office is investigating why New Jersey−based Medco Health Solutions waited six weeks to notify Ohio officials of a serious data breach after Social Security numbers of 4,000 state workers and their dependents were stolen on December 28. (See item 15)
- The Associated Press reports Arizona authorities are concerned that a small plane stolen from an airport in Marana was apparently flown to Mexico. (See item 21)
- The Associated Press reports the U.S. government is buying 12.4 million more doses of Tamiflu, a drug that can lessen the severity of bird flu, for the nation's stockpile. (See item 28)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *March 02, PPL Susquehanna* — **Alert ends at PPL's Susquehanna nuclear power plant.** The alert at PPL's Susquehanna nuclear power plant in Luzerne County, PA, ended at 4:33 a.m. EST Thursday, March 2. The plant continues to operate normally. There was no release of radiation and an investigation continues to find the cause of the incident. The alert was declared after a

fire protection system activated in a building located in a non−nuclear area of the plant. The plant's fire brigade responded to the building after the system activated and found no fire. PPL is investigating why the fire protection system activated, releasing halon gas. "The plant remained safe and secure throughout the incident," said Miriam Mylin, public information manager for PPL Susquehanna. The alert was declared at 9:27 p.m. EST Wednesday, March 1. An alert is the second lowest of four emergency classifications for U.S. nuclear power plants established by the Nuclear Regulatory Commission. PPL notified Luzerne and Columbia county emergency management agencies, as well as the Pennsylvania Emergency Management Agency. The company also has notified the Nuclear Regulatory Commission.
Source: http://biz.yahoo.com/prnews/060302/nyth099.html?.v=43

2. *March 02, Casper Star−Tribune (WY)* — **Pipeline adds years to Wyoming's gas boom.** Construction of a massive new pipeline from the Rockies to markets in the eastern United States will show that Wyoming's natural gas boom isn't about to slow down anytime soon, according to industry experts. The Rockies Express Pipeline will give natural gas producers in Wyoming, Colorado, and Utah an additional 1.8 billion cubic feet of access to one of the most lucrative markets in the nation. "Rockies Express will help insulate Wyoming from the boom−and−bust cycles it has dealt with in the past and help assure steady, consistent growth," said Bryan Hassler of the Wyoming Natural Gas Pipeline Authority. The Rockies' natural gas ramp−up comes as production from older natural gas fields in the Gulf Coast states declines. Construction is already under way on a pipeline from Meeker, CO, to Wamsutter, where BP has a 15−year plan to drill 2,000 new deep gas wells. Rockies Express will open export capacity incrementally until it is in full service in 2009. EnCana plans to drill an additional 3,200 wells in the Jonah Field near Pinedale, coal−bed methane producers have tapped only five percent of the Powder River Basin, and Anadarko Petroleum is planning a drilling program in southern Wyoming.
Source: http://www.casperstartribune.net/articles/2006/03/02/news/wyoming/e35a15d86893e0f0872571240004cdbb.txt

3. *March 01, Houston Business Journal (TX)* — **Nigerian militants release five more Willbros workers.** Five more of the nine Willbros Group Inc. workers taken hostage 11 days ago by Nigerian militants have been freed. Willbros said Wednesday, March 1 that the five are in addition to Macon Hawkins, an American from Texas, who the company announced earlier Wedenesday was the sole freed hostage. The Houston−based independent contractor is working with authorities to continue to secure the safe return of its three remaining employees: two Americans and one British national working as a security expert for a private firm under contract to Willbros. The incident has interrupted three projects Willbros was working on in the area and has forced a 20 percent reduction in Nigerian crude exports. The militants on February 18 blew up two oil and gas pipelines and set fire to a tanker loading platform at Royal Dutch Shell's Forcados oil terminal, shutting down a stream of more than 500,000 barrels of oil a day.
Source: http://www.bizjournals.com/industries/energy/oil_gas/2006/02/27/houston_daily32.html

4. *March 01, Associated Press* — **Alliant Energy sells three power plants.** Alliant Energy Corp. said Wednesday, March 1 it has completed the sale of three power plants in China to a company in Thailand. Alliant sold the plants to Banpu PLC and was released from its $15 million of debt associated with the plants. The Madison−based power company expects to sell a

fourth plant in China by June. Alliant said it is selling off its overseas investments to focus on domestic customers in Wisconsin and Iowa.
Source: http://news.yahoo.com/s/ap/20060301/ap_on_bi_ge/alliant_plan t_sales_1

5. *February 28, Los Alamos Monitor (NM)* — **Lawrence Livermore National Laboratory cited for nuclear safety breach.** The National Nuclear Security Administration (NNSA) plans to issue a citation for a series of safety violations that began in April 2004 at Lawrence Livermore National Laboratory (LLNL) in Livermore, CA. The violations include multiple radiological exposures. Los Alamos National Laboratory was last cited in June 2004 for an event in which five workers were seriously exposed to toxic vapors. In January 2005, in the midst of a laboratory−wide shutdown at Los Alamos National Laboratory, LLNL ordered a standdown of its plutonium facility as a result of complications related to the current set of violations. Two draft plans to resolve the safety issues at Livermore's plutonium facility were rejected by the NNSA supervisors at Livermore, triggering the standdown. Two separate exposures were penalized, including a radiological uptake involving a Mobile Visual Examination and Repackaging Unit and a radiological spill involving phosphorous−32. The spilled chemical was carried home on the shoe of an exposed worker.
Source: http://www.lamonitor.com/articles/2006/02/28/headline_news/n ews02.txt

6. *February 27, Fortune Magazine* — **Royal Dutch Shell depleting oil reserves.** Analysts are worried that buried beneath Royal Dutch Shell's record profit figures are worrying signs of a business in decline. Shell hasn't been able to find nearly as much oil and gas as it's now pumping out of the ground. In fact, it hasn't even come close −− replacing only 60 percent to 70 percent of what it produced in 2005 and only 19 percent in 2004. Troubling Shell now is that the company is falling way behind rivals like Exxon and BP despite spending billions more each year on exploring and drilling new wells. Last year Exxon replaced 112 percent of production, and BP came up with 95 percent. Fadel Gheit of Oppenheimer & Co. says, "I have never seen anything like this...Shell used to represent the gold standard in this industry, but lately they can't get their act together." Shell still has huge assets −− nearly 12 billion barrels, but reserve replacement is the best guide to whether a company will be able to maintain −− or grow −− production in the future. Shell's daily production figures have been weak lately, falling 6.7 percent in 2005, to 3.52 million barrels a day.
Source: http://money.cnn.com/2006/02/27/magazines/fortune/shell_fort une/index.htm

[Return to top]

Chemical Industry and Hazardous Materials Sector

7. *March 02, Associated Press* — **Propane leak shuts down much of downtown Vermont city.** A leaky propane tank at a downtown coin−operated laundry Wednesday, March 1, prompted firefighters to close a four−block part of Rutland, VT, to traffic. The leak was fixed in about a half an hour.
Source: http://www.boston.com/news/local/vermont/articles/2006/03/02 /propane_leak_shuts_down_much_of_downtown_rutland/

8. *March 02, Chicago Tribune* — **Hospital chemical spill sends 15 to emergency room,**

prompts road closure. A chemical spill of ethylene oxide in the basement of St. Mary of Nazareth Hospital Center in Wicker Park, IL, Thursday morning, March 2, sent about 15 people to its emergency room as a precaution. The chemical leaked from a canister used for a sterilization machine. Traffic was blocked off on several streets surrounding the area. No evacuations were required.
Source: http://www.chicagotribune.com/news/custom/newsroom/chi-06030 2chemicalspill,1,7233442.story?coll=chi-news-hed

[Return to top]

Defense Industrial Base Sector

9. *March 01, Government Accountability Office* — **GAO-06-478T: Defense Acquisitions: Business Case and Arrangements Key for Future Combat System's Success (Testimony).** The Future Combat System (FCS) is a networked family of weapons and other systems in the forefront of efforts by the Army to become a lighter, more agile, and more capable combat force. When considering complementary programs, projected investment costs for FCS are estimated to be on the order of $200 billion. FCS's cost is of concern given that developing and producing new weapon systems is among the largest investments the government makes, and FCS adds significantly to that total. Over the last five years, the Department of Defense doubled its planned investments in such systems from $700 billion in 2001 to $1.4 trillion in 2006. At the same time, research and development costs on new weapons continue to grow on the order of 30 to 40 percent. FCS will be competing for significant funds at a time when Federal fiscal imbalances are exerting great pressures on discretionary spending. In the absence of more money being available, FCS and other programs must be executable within projected resources. In this testimony, Paul L. Francis, Director of Acquisition and Sourcing Management, discusses (1) the business case needed for FCS to be successful and (2) related business arrangements that support that case.
Highlights: http://www.gao.gov/highlights/d06478thigh.pdf
Source: http://www.gao.gov/cgi-bin/getrpt?GAO-06-478T

10. *March 01, Reuters* — **Army defends $125 billion communications program.** U.S. Army officials on Wednesday, March 1, said a $125 billion communications modernization program is on track for a key Pentagon review in May, despite delays in two other programs that are needed to run its extensive communications networks. The Future Combat Systems program will use advanced communications to give troops more information by linking 18 light, fast, manned and robotic air and ground vehicles. It will be rolled out over two decades. Army acquisition chief Claude Bolton told a Senate Armed Services Committee subcommittee that 2006 is a "critical execution year" for the program. It faces more than 52 reviews, key hardware and software deliveries, and several field experiments this year, he said.
Source: http://today.reuters.com/News/newsArticle.aspx?type=politics News&storyID=2006-03-01T195524Z_01_N01239120_RTRUKOC_0_US-AR MS-BOEING-ARMY.xml

11. *March 01, U.S. Army* — **Army '07 budget boosts FCS, irregular warfare.** The Army will get $111.8 billion of the requested 2007 Department of Defense (DoD) budget, including a nearly $4 billion boost to future combat systems, such as unmanned aerial vehicles. Close to 50

percent of the Army's requested budget for Fiscal Year 2007 will go toward personnel−related areas of military, civilian manpower and retiree pay, according to the assistant secretary of the Army for Financial Management and Comptroller. The Army's investment focus, according to Comptroller officials, is in line with the overall theme of the DoD budget for 2007, which prioritizes the capabilities of irregular warfare operations, defending American soil against advanced threats, maintaining America's military superiority, and supporting service members and their families.
Source: http://www4.army.mil/ocpa/read.php?story_id_key=8641

12. *March 01, Congress Daily* — **Air Force presses case for faster replacement of tankers.** Air Force officials told House lawmakers Tuesday night, February 28, they want to proceed this year with expensive plans to replace its fleet of KC−135 aerial refueling tankers, despite a recent analysis that found the 1950s−era planes can fly for another quarter century. If the Air Force does not begin to replace the fleet now, the service may end up flying many of these tankers, which lack defenses and other systems, for another 40 years. According to Lt. Gen. Donald Hoffman, the service's top acquisition officer, and other officials, the planes are aging and experiencing problems that could hinder operations. Meanwhile, the cost of maintaining the fleet is increasing rapidly as the planes' capabilities decline.
Source: http://www.govexec.com/story_page.cfm?articleid=33484&dcn=to daysnews

[Return to top]

Banking and Finance Sector

13. *March 02, VNUNet* — **Identity theft victims to sue NCsoft.** Lawyers in South Korea have filed a class action lawsuit on behalf of more than 230,000 victims of identity theft in an online game. The suit will claim damages of about $1,000 for each plaintiff whose identity was used to register new accounts in NCsoft's popular games, Lineage and Lineage 2, according to media reports. Most of the identify thefts took place over the past six months as underground gaming syndicates stole victims' official Korean ID numbers in hacking attacks and used them to register hundreds of thousands of Lineage accounts. The new accounts were then 'farmed' by low paid workers in Chinese gaming sweatshops to generate 'gold' and other game−world items that could be sold for real world cash. NCsoft has claimed that it registered the bogus accounts in good faith, and has denied responsibility for the initial theft of ID numbers that made the crime possible. As well as Lineage, which claims millions of players worldwide, NCsoft operates popular games like City of Heroes, City of Villains, and Guild Wars in Europe and the U.S., and plans to release the much−anticipated Auto Assault this summer.
Source: http://www.vnunet.com/articles/print/2151224

14. *March 02, Finextra* — **Majority of British bank online.** Over half of British adults −− 59 percent −−now use online banking services to manage their finances, according to research commissioned by the UK's Alliance and Leicester (A&L). A survey of 2,395 UK adults conducted by research firm YouGov found that two thirds (61 percent) are using Internet banking a lot more than they did two years ago, with 12 percent using the services once a day. A&L says its own research found that the most popular reasons for accessing online services is to check balances (96 percent), followed by making payments and fund transfers (76 percent). Furthermore, three quarters of its customers (74 percent) say they find Web banking more

convenient than using a branch. Of those not currently using Web banking, A&L says its statistics show 21 percent prefer dealing directly face−to−face with staff, while 13 percent say they have reservations for security reasons. However, 29 percent says a security guarantee would be likely to encourage them to use online services more.
Source: http://www.finextra.com/fullstory.asp?id=14993

15. *March 01, Computerworld* — **Vendor waited six weeks to notify Ohio officials of data breach.** The Ohio state attorney general's office is investigating the terms of a contract between the state Department of Administrative Services and Medco Health Solutions Inc., a New Jersey−based prescription drug benefits provider, after a laptop computer containing the unencrypted Social Security numbers and birth dates of about 4,300 state workers and 300 of their dependents was stolen on December 28. Ben Piscitelli, a spokesperson for the Ohio Department of Administrative Services (DAS), said the laptop was stolen from the home of a Medco employee. Medco officials waited until February 8 to inform the state about the theft. "We told them that delay was unacceptable," Piscitelli said. The laptop computer contained the prescription benefits membership numbers −− which are the same as employee Social Security numbers −− of the state employees and dependents. Birth dates and details about the drugs the patients were taking were also in the data records. The data did not include names or addresses of the affected persons. Piscitelli said, "Our concern is that the state can't gamble" with such data losses. The agency has received no reports of identity theft or credit fraud from any of the persons affected by the incident.
Source: http://www.computerworld.com/securitytopics/security/story/0 ,10801,109116,00.html

16. *March 01, eWeek* — **Hacker outsmarts Kinko's ExpressPay cards.** A security hole in a common technology used to manage prepaid store cards could let malicious hackers and other criminal groups bilk FedEx Kinko's stores, according to a recently published report. A security hole could allow hackers to clone legitimate cards or change the value of a card to any amount, according to Strom Carlson, a hardware security researcher at Secure Science in San Diego. The report is just the latest warning about vulnerabilities in cash card technology, which is becoming a popular tool for money laundering, according to one banking fraud expert. According to the report, data stored on the cards is not encrypted and can be viewed by anyone with a magnetic card reader. Data on the card can be modified with a security code, said Carlson. Carlson said he purchased a Kinko's card for $1, and then wired it to a USB logic analyzer that sniffed the secret code from an ExpressPay card as it interacted with the kiosk. Malicious hackers could gain almost unlimited access to Kinko's store resources with the cards, because they can purchase, recharge, and use them without interacting with store employees, he said.
Source: http://www.eweek.com/print_article2/0,1217,a=172554,00.asp

17. *March 01, U.S. Department of Justice* — **Three Oklahoma residents indicted for conspiring to defraud FEMA of Hurricane Katrina relief funds.** Three Oklahomans have been indicted for conspiring to defraud the U.S. of Hurricane Katrina disaster relief funds and stealing Federal Emergency Management Agency (FEMA) funds, United States Attorney John C. Richter announced Wednesday, March 1. He said, "The Hurricane Katrina Fraud Task Force has charged over 210 individuals who have greedily sought to exploit others' suffering for their personal benefit." The defendants charged in the superseding indictment, Sheila A. Perry, 38; Atari Finley, 26; and Michael A. Young, 27, are all from Lawton, OK. According to the

superseding indictment, all three defendants were involved in a conspiracy in September and October of 2005 to obtain $2,000 Hurricane Katrina disaster relief payments through FEMA's Internet Website for individuals who were not eligible for or entitled to those funds. The superseding indictment alleges that Perry and Finley recruited other conspirators, who were required to provide a portion of the proceeds of disaster assistance payments in their names to Perry or Finley in exchange for the opportunity to participate in the scheme.
Source: http://releases.usnewswire.com/GetRelease.asp?id=61717

[Return to top]

Transportation and Border Security Sector

18. *March 02, Associated Press* — **Woman drives car onto Dulles airport.** A woman drove her car onto private airport property at Washington Dulles International Airport on Wednesday afternoon, March 1, passing through two manned checkpoints before she was stopped, authorities said. "From the time she went through the first manned checkpoint, she was followed by airport operations officers and security guards and was brought to a stop quickly," said Tara Hamilton, a spokesperson for the Metropolitan Washington Airports Authority. "Police arrived immediately and she was placed under arrest."
Source: http://www.usatoday.com/travel/flights/2006−03−02−dulles−bre ach_x.htm

19. *March 02, Department of Transportation* — **New federal rule aims to reduce human error as cause of train accidents.** Visiting a railroad employee training facility in Atlanta, GA, Federal Railroad Administration Administrator Joseph H. Boardman announced on Thursday, March 2, that his agency intends to issue regulations to address the most common human errors that cause train accidents. The Federal Railroad Administration (FRA) is accelerating development of a rule that will focus on reducing the most common human errors such as improperly lined track switches, shoving or pushing rail cars without properly monitoring for safe conditions, and leaving rail cars in a position that obstruct an adjacent track, Boardman said. The proposed regulations will be published by September 2006. “The new regulation will provide additional enforcement authority over violations of common operating practice errors,” said Boardman. “This effort is one of many aggressive steps we are taking to prevent train accidents from occurring in the first place,” he added. Human factors are the leading cause of train accidents, accounting for 38 percent of the total, Boardman said. The new rule would be the first significant update of Federal regulations governing railroad employee adherence to operating rules. The FRA also is actively working on other initiatives to reduce human factor−caused train accidents, and research to address railroad worker fatigue.
Source: http://www.dot.gov/affairs/fra0206.htm

20. *March 02, Lansing State Journal (MI)* — **Canadian trash trucks may be threat to safety.** In addition to being a stinky nuisance and an environmental hazard, Canadian trash trucks coming to Michigan also could pose terrorist threats, a recently released Department of Homeland Security (DHS) report shows. Fewer than 10 of the 415 trash trucks that come into Michigan each day from Ontario are physically inspected by Customs and Border Protection agents. That would make it easy for terrorists to smuggle chemical or biological materials into the state. Screening Trucks Carrying Canadian Municipal Solid Waste (DHS Unclassified Summary) OIG−06−21, updated on February 27:

http://www.dhs.gov/dhspublic/interapp/editorial/editorial_03 34.xml
Source: http://www.lsj.com/apps/pbcs.dll/article?AID=/20060302/NEWS01/603020349/1001/news

21. *March 02, Associated Press* — **Stolen plane may have been flown to Mexico.** Arizona authorities suspect that a small plane stolen from an airport in Marana may have been flown to Mexico. The 1966 Cessna Skylane was stolen Tuesday morning, February 28, from Marana Regional Airport in Marana, AZ, which is about 90 miles north of the border. Marana Police Department spokesperson Sgt. Jose Alvarez said the thief removed a padlock from a locked hangar and stole the small aircraft, worth about $120,000. Alvarez said Marana police were informed by the Federal Aviation Administration that a small aircraft was seen leaving the Marana airport. It flew at a low altitude toward another small airport and crossed the border into Mexico near Nogales. "We took it as a threat because it was flown into Mexico," Alvarez said.
Source: http://www.azcentral.com/news/articles/0302StolenPlane02−ON. html

[Return to top]

Postal and Shipping Sector

22. *March 02, DMNews* — **Domestic ground parcel shipments on pace for record.** The U.S. domestic ground parcel category is headed for a record year in 2005 with shipments poised to exceed four billion for the first time and with revenue approaching $25 billion, the Colography Group Inc. said on Wednesday, March 1, in its third−quarter and nine−month 2005 analysis report. The report also found that domestic regional less−than−truckload (LTL) carriers continued to gain share of the LTL market, holding 82 percent of shipments as of September 2005 versus 78.5 percent at the end of fourth−quarter 2004. Domestic ground parcel revenue through the first nine months exceeded $19.2 billion. The report credited DHL Express with the most impressive performance through 2005's first nine months. Ted Scherck, president of The Colography Group, said, "Regional LTL and ground parcel activity continued strong while national LTL struggled to hold share…. U.S. shipping has moved to a regionally based, surface−driven model, and there is no turning back." The Report also indicated that much of the overall gains apparently came at the expense of the U.S. Postal Service, whose market share fell from 11.4 percent by the end of Q4 2004 to 8.4 percent at the end of third−quarter 2005.
Colography Group Website: http://www.colography.com/nationalsrvy.html
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=3592 8

[Return to top]

Agriculture Sector

23. *March 02, USAgNet* — **Missouri Farm Bureau offers reward for cattle thieves.** In response to the growing number of cattle thefts in the state, Missouri Farm Bureau is offering a $5,000 reward for information that leads to the arrest and conviction of individuals committing a felony in the theft of cattle from Farm Bureau members. Since the first of the year, hundreds of cattle have been reported as stolen in Missouri. Currently, Missouri Farm Bureau has a $2,000 reward program which applies to the theft of any of its members' property. For a period of time

as deemed necessary, Farm Bureau is increasing this reward program for cattle theft to $5,000.
Source: http://www.usagnet.com/story−national.cfm?Id=307&yr=2006

24. *February 28, Associated Press* — **Sweden reports suspected case of mad cow disease.** Sweden reported a suspected case of mad cow disease after tests showed symptoms of the illness in a domestic cow, authorities said Tuesday, February 28. The tests from a 12−year−old cow in central Sweden had been sent to a laboratory in the United Kingdom for confirmation, the Vastmanland county government said in a statement. Sweden is one of few European countries that have never had a confirmed case of mad cow disease, or bovine spongiform encephalopathy.
Source: http://www.cattlenetwork.com/content.asp?contentid=19949

[Return to top]

Food Sector

25. *March 01, Associated Press* — **Number of people sickened in sushi food poisoning case rises.** Health officials have received 123 reports from people who say they became ill after eating at a sushi restaurant in Bentonville, AR, and the reports keep coming in. The restaurant remained closed Tuesday, February 28 after a salmonella outbreak. Ann Wright, a spokesperson with the Arkansas Department of Health and Human Services, said the department's lab has confirmed 30 cases. The cases were connected to the restaurant because of statements given by people who became sick, but food taken from the restaurant tested negative for salmonella. Wright said the cause of the outbreak may never be known.
Source: http://www.thehometownchannel.com/news/7586153/detail.html

[Return to top]

Water Sector

26. *March 02, Kansas City Star (MO)* — **Drought cancels water release.** Winter drought has canceled a water release this month for the Missouri River. Reservoir levels in the Dakotas and Montana, lowered by years of drought, are below the level required to allow extra water releases to boost spawning by pallid sturgeon, Corps of Engineers spokesperson Paul Johnston said Wednesday, March 1. Spring runoff from mountain snow is expected to be 80 percent of normal, with reservoirs already at record lows. A spring rise still will occur as the corps begins increasing water releases in late March for the barge navigation season, which begins April 1. But a two−day pulse on top of those releases is canceled. Even with the pulse, Johnston said, water levels would still have been below normal navigation levels. A pulse is planned for May, he said, but only if lake levels rise.
Source: http://www.kansascity.com/mld/kansascity/news/local/13994696 .htm

27. *March 02, China Daily* — **Ocean reservoir to tackle water shortage.** An "ocean reservoir" could be built to help alleviate future water shortages in Shenzhen, China. The city's water supply capability currently stands at 1.9 billion cubic meters of water a year. But researchers believe it may need an extra 360 million cubic meters in 2010, one billion cubic meters in 2020,

and 1.4 billion cubic meters in 2030 to support the normal operation of its fast−growing society. The statistics are from the nation's first government−organized study that comprehensively addresses the water problem. The report suggests looking at the feasibility of building a reservoir, which could contain 200 million cubic meters of water, in the sea off eastern Shenzhen. It would collect a large quantity of fresh water before it runs into the sea. It would need a type of membrane that could separate the fresh water from the salty water in the sea. Currently, a number of Chinese cities, including Macao and Shanghai, have set up such reservoirs but the one in Shenzhen, if implemented, would be the country's largest−scale reservoir in the sea.
Source: http://www.chinadaily.com.cn/english/doc/2006−03/02/content_525403.htm

[Return to top]

Public Health Sector

28. *March 01, Associated Press* — **More Tamiflu ordered for federal stockpile.** The U.S. government is buying more Tamiflu, a drug that can lessen the severity of bird flu, for the nation's stockpile. Already on hand is enough of the drug to treat about five million people. On Wednesday, March 1, the government ordered from the manufacturer enough to treat 12.4 million more. The purchases are part of government preparations in case the bird flu, or some other strain of influenza, one day sparks a worldwide epidemic.
Source: http://www.usatoday.com/news/health/2006−03−01−tamiflu_x.htm ?POE=NEWISVA

29. *March 01, Reuters* — **Lab network proposed to avert bird flu pandemic.** A global network of laboratories modeled on existing U.S. military facilities could help to avert an influenza pandemic, scientists said on Wednesday, March 1. Researchers from the U.S. Department of Defense Global Emerging Infections Surveillance and Response System (DoD−GEIS) said the facilities would improve preparedness against bird flu and other emerging infections in poor regions such as sub−Saharan Africa. The U.S. Naval Medical Research Unit−2 (NAMRU−2) in Jakarta, Indonesia, helped to detect avian influenza there last summer. Another unit in Egypt was essential in spotting cases of the virus in humans in Turkey and Iraq, according to the scientists. Both units were among many set up decades ago. But due to budget cuts and other reasons, labs in Panama, Puerto Rico, Brazil, Congo, Uganda, Ethiopia, and Malaysia have been closed. The current DoD−GEIS influenza surveillance network includes sites in more than 20 countries.
Source: http://www.alertnet.org/thenews/newsdesk/L28748095.htm

30. *February 28, Reuters* — **Australian scientists test Nipah virus vaccine.** Australian scientists are testing a vaccine to fight two deadly animal viruses that can infect and kill humans. Scientists say one of the pathogens, the Nipah virus, is considered a potential biological weapon. It killed more than 100 people and a million pigs in Malaysia in 1999, while the Hendra virus killed two Australians in 1994. The Nipah virus is a member of a new genus of viruses related to the mysterious Hendra virus, which killed two people and 16 horses in Australia's northern state of Queensland in 1994−95. Both viruses are carried by fruit bats and have alarmed scientists with the ease in which they jump from animals to humans. Scientists from the Australian government's Commonwealth Scientific and Industrial Research Organization (CSIRO) said on Tuesday, February 28, that testing of a new vaccine showed

promise of preventing both diseases.
Nipah and Hendra virus information:
http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/nipah.ht m
Source: http://today.reuters.com/news/newsArticle.aspx?type=scienceN ews&storyID=2006−02−28T061903Z_01_SYD150672_RTRUKOC_0_US−NIP AH−VACCINE.xml

[Return to top]

Government Sector

31. *March 02, Government Accountability Office* — **GAO−06−253T: Social Security Administration: Procedures for Issuing Numbers and Benefits to the Foreign−Born (Testimony).** In 2004, an estimated 35.7 million foreign−born people resided in the United States, and many legitimately have Social Security numbers. Many of these individuals have Social Security numbers (SSNs), which can have a key role in verifying authorization to work in the United States. However, some foreign−born individuals have been given SSNs inappropriately. Recent legislation, aimed at protecting the SSN and preventing fraud and abuse, changes how the Social Security Administration (SSA) assigns numbers and awards benefits for foreign−born individuals. The chairman of the Subcommittee on Social Security asked the Government Accountability Office (GAO) to address two questions. First, how does SSA determine who is and is not eligible for an SSN? Second, how does SSA determine who is and is not eligible for Social Security benefits? GAO is making no new recommendations in this testimony.
Highlights: http://www.gao.gov/highlights/d06253thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−253T

[Return to top]

Emergency Services Sector

32. *March 02, Seattle Post−Intelligencer (WA)* — **Washington tests voice−over−Internet calls for first responders.** Washington's Emergency Management Division is testing a new mobile communications system that uses voice−over−Internet connections by satellite −− a technology that could allow firefighters, police and other emergency personnel to talk with one another even if cellular, telephone or radio networks are damaged or non−existent. Built last summer, the $175,000 mobile communications unit will be tested during a tsunami exercise at Camp Rilea, OR, in the next couple of months. The 12−foot trailer includes a satellite dish, collapsible radio antenna and numerous power supplies. The goal is to have the trailer in use during the wildfire season this summer, providing voice, video and data connectivity to supervisors and incident commanders in remote areas. The system also includes a VHF−AM radio, so firefighters on the ground can instruct air crews where to drop water.
Source: http://seattlepi.nwsource.com/business/261392_disaster02.htm l

33. *March 01, Air Force Link* — **Guard tests world's first multi−person rescue basket.** An Air National Guard rescue unit successfully tested the world's first multi−person rescue basket, a

cage−like device that, once certified, can carry up to 15 people. The Heli−Basket is a four−and−a−half foot by eight−and−a−half foot metal cage that hangs on a 125−foot cable below an HH−60G Pave Hawk helicopter. The inventor, John Tollenaere, said it was the first time a rescue device like his has been tested for human use. Using a litter or a harness, para−rescuemen normally only rescue one person at a time. In extreme circumstances, they can rescue two people if all three's combined weight is not more than 600 pounds. The Heli−Basket's can carry up to 8,800 pounds.
Source: http://www.af.mil/news/story.asp?id=123016794

34. *March 01, Honolulu Adviser (HI)* — **Department of Defense hosts avian flu drill in Hawaii.** In an avian flu drill scenario conducted Tuesday, February 28, in Hawaii: A human−transmitted avian flu outbreak occurs in Thailand which eventually spreads to Honolulu and the Mainland. The exercise time frame covered 14 weeks and used news reports, videos and graphics to show the spread to Honolulu and other major port cities before the disease moved farther inland. The drill's objectives involved maintaining vital operations of services such as water, sewer and roads, keeping government running and deciding priorities for using any available vaccines and antiviral drugs.
Source: http://www.honoluluadvertiser.com/apps/pbcs.dll/article?AID=/20060301/NEWS15/603010352/1026/NEWS

35. *March 01, Washington Technology* — **New Safecom requirements play up wireless for first responders.** Wireless networks will take on a much more prominent role in the Department of Homeland Security's updated requirements for interoperable communications for first responders. The Safecom program, which is the departmental unit promoting improved radio communications for emergency response agencies, has released a 208−page "Statement of Requirements for Public Safety Wireless Communications & Interoperability" (Version 1.1) on its Website. The new requirements address all manner of wireless networks, from personal and temporary to huge, extended systems.
Safecom's Statement of Requirements, Version 1.1:
http://www.safecomprogram.gov/SAFECOM/library/technology/124 6_statementof.htm
Source: http://www.washingtontechnology.com/news/1_1/daily_news/2811 7−1.html

[Return to top]

Information Technology and Telecommunications Sector

36. *March 01, FrSIRT* — **Apple Mac OS X code execution and denial−of−service vulnerabilities.** Apple has released security updates to address multiple vulnerabilities identified in Mac OS X. Analysis: These flaws could be exploited by remote or local attackers to execute arbitrary commands, bypass security restrictions, disclose sensitive information, or conduct cross site scripting and denial−of−service attacks. See source advisory for vulnerability details. Affected products: Mac OS X version 10.3.9, Mac OS X Server version 10.3.9, Mac OS X version 10.4.5, Mac OS X Server version 10.4.5.
Solution: Security Update 2006−001 for Mac OS X 10.4.5 (PPC):
http://www.apple.com/support/downloads/securityupdate2006001 macosx1045ppc.html
Security Update 2006−001 for Mac OS X 10.4.5 Client (Intel):
http://www.apple.com/support/downloads/securityupdate2006001 macosx1045clientintel.html

Security Update 2006−001 for Mac OS X 10.3.9 Client:
http://www.apple.com/support/downloads/securityupdate2006001_1039client.html
Security Update 2006−001 for Mac OS X 10.3.9 Server:
http://www.apple.com/support/downloads/securityupdate2006001_1039server.html
Source: http://www.frsirt.com/english/advisories/2006/0791

37. *March 01, FrSIRT* — **Sun security update fixes multiple Apache Web server vulnerabilities.** A vulnerability in the Apache 1.3 Web server bundled with Solaris 8 and 9 may allow a local user who is able to create e SSI documents which are served by Apache to execute arbitrary code with the privileges of the Apache 1.3 process. The Apache HTTP process normally runs as the unprivileged user "nobody" (uid 60001). Analysis: This vulnerability affects the Apache 1.3 Web server bundled with Solaris 10 which may prevent certain configured security features from being applied to specific HTTP transactions when Apache is configured to use SSL. The second vulnerability in the Apache 1.3 Web server may allow local or remote unprivileged users to bypass security protections associated with some network transactions, corrupt information stored in a Web cache, or perform cross site scripting activities when the Apache Web server is configured to run as a proxy. Affected products: Sun Solaris 8, Sun Solaris 9, and Sun Solaris 10.
Solution: Until patches are available, upgrade to the latest versions of Apache and mod_ssl as an interim workaround.
Source: http://www.frsirt.com/english/advisories/2006/0789

38. *March 01, FrSIRT* — **IBM WebSphere Application Server source code disclosure vulnerability.** A vulnerability has been identified in IBM M WebSphere Application Server, which can be exploited by remote attackers to gain knowledge of sensitive information. Analysis: The flaw is due to an input validation error when processing malformed HTTP requests containing a specially crafted filename extension, which could be exploited by remote attackers to display the source code of arbitrary JavaServer pages (JSP) instead of an expected HTML response. Affected products: IBM WebSphere Application Server version 5.1.1.4 through 5.1.1.9; IBM WebSphere Application Server version 5.0.2.10 through 5.0.2.15.
Solution: Upgrade to version 5.0.2.16 or 5.1.1.10 (when available) or apply Interim fixes:
http://www−1.ibm.com/support/docview.wss?rs=180&uid=swg2_7004980
Source: http://www.frsirt.com/english/advisories/2006/0788

39. *March 01, Security Tracker* — **Oracle E−Business Suite 'Oracle Diagnostics' bugs let remote users access functions and inject SQL commands.** A vulnerability was reported in Oracle E−Business Suite. A remote user can access diagnostic functions and can inject SQL commands. Analysis: The Oracle Diagnostics Webpages and Java classes in Oracle E−Business Suite contain several vulnerabilities. A remote user can access some of the diagnostic functions. A remote user can also inject SQL commands. There are some permission errors may let remote users access functions or data without authorization. Affected version: 11i.
Solution: The vendor has issued the following fix: "Diagnostics Support Pack February 2006 with Oracle Diagnostics 2.3 RUP A." The fix will be included in the next quarterly Critical Patch Update (April 18, 2006).
Source: http://securitytracker.com/alerts/2006/Mar/1015699.html

40.

March 01, Tech Web — **Mystery over PC−to−mobile Trojan annoys researchers.** Anti−virus researchers complained Wednesday, March 1, that a group claiming to have proof of the first PC−to−mobile Trojan hasn't shared the sample, a normal practice among security investigators. Monday, February 27, the Mobile Antivirus Researchers Association (MARA), which bills itself as a non−commercial collection of mobile malware researchers, said it had anonymously received malicious code it dubbed "Crossover." The sample, said MARA, could cross−infect a Windows Mobile Pocket PC from a desktop PC running Windows. According to MARA, the first−of−its−kind Trojan spreads to the mobile device via Microsoft's ActiveSync, then erases all files in the My Documents directory of the Windows CE− or Windows Mobile−based gizmo. But unlike the usual practice where virus researchers share samples, MARA's not willing to let others see the code, no−strings−attached, say some commercial researchers. They're left without a way to confirm Crossover's existence or MARA's claims, or update their own signatures to defend against the attacker.
Source: http://www.securitypipeline.com/news/181401932

41. *March 01, F−Secure* — **New F−Secure world virus map offers current global perspective at a glance.** F−Secure has launched a comprehensive online tool for those interested in understanding the world virus situation at a glance. The resource, which was developed for research purposes at F−Secure is now available to the general public in four languages, respectively English, French, German and Finnish.
F−Secure World Map: http://worldmap.f−secure.com/vwweb_1_2/en/previous_day
Source: http://www.f−secure.com/news/items/news_2006030101.shtml

42. *March 01, Federal Computer Week* — **DHS wireless experiment takes to orbit.** A Department of Homeland Security (DHS) experiment testing wireless communications and infrastructure is moving into a new phase, said Douglas Maughan, the project's program manager at the Homeland Security Advanced Research Projects Agency. Maughan said the project involves 15 Canadians and 25 Americans at DHS. The effort involves sending about 1,000 wireless messages a day to test security products and other parameters, some sent by the participants and others with an automated system. This summer, the project will shift from testing cellular communications to satellite communications.
Source: http://www.fcw.com/article92459−03−01−06−Web

43. *March 01, Federal Computer Week* — **OMB delivers positive IT security report.** The Office of Management and Budget (OMB) Wednesday, March 1, presented its report, “FY2005 Report to Congress on Implementation of the Federal Information Security Management Act of 2002,” to Congress. The report showed steady progress in closing security gaps in federal agencies. It found that 85 percent of IT systems to be certified and accredited and that the quality of the certifications and accreditations at the agencies also increased.
OMB's report: http://www.whitehouse.gov/omb/inforeg/reports/2005_fisma_report_to_congress.pdf
Source: http://www.fcw.com/article92474−03−01−06−Web

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available exploit code for a vulnerability in Apple Safari Browser. The Apple Safari browser will automatically open "safe" file types, such as pictures, movies, and archive files. A system may be compromised if a user accesses an HTML document that references a specially crafted archive file. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary commands with the privileges of the user.

More information can be found in the following US−CERT Vulnerability Note:

VU#999708 − Apple Safari may automatically execute arbitrary shell commands
http://www.kb.cert.org/vuls/id/999708

Although there is limited information on how to fully defend against this exploit, US−CERT recommends the following mitigation:

Disable the option "Open 'safe' files after downloading," as specified in the Securing Your Web Browser document.

Current Port Attacks

Top 10 Target Ports	6881 (bittorrent), 1026 (win−rpc), 25 (smtp), 445 (microsoft−ds), 55620 (−−−), 32459 (−−−), 4142 (oidocsvc), 139 (netbios−ssn), 3800 (−−−), 5817 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

44. *March 02, Steubenville Herald−Star (OH)* — **Bomb threats cause two Ohio plant evacuations.** Two Salem−area manufacturing plants were evacuated just before noon Monday, February 27, after an unidentified caller claimed there were bombs at both facilities. No bombs were found at either Sekely Industries or Quaker Manufacturing, and work resumed at both facilities after emergency personnel determined the call most likely was a hoax. Investigators are working to determine who made the bomb threat. Salem police Sgt. John Less said the county Sheriff's Department dispatcher received the call through 911. The male caller claimed bombs would go off at both facilities 10 minutes later, and the dispatcher immediately notified police in Salem and Perry Township. Less said the caller identification at the Sheriff's Department provided police with a number for the phone used to make the bomb threat, and he

was able to trace the call to the pay phone at the Quaker Village.
Source: http://www.morningjournalnews.com/news/story/032202006_new02 news21.asp

[Return to top]

General Sector

Nothing to report.
[Return to top]